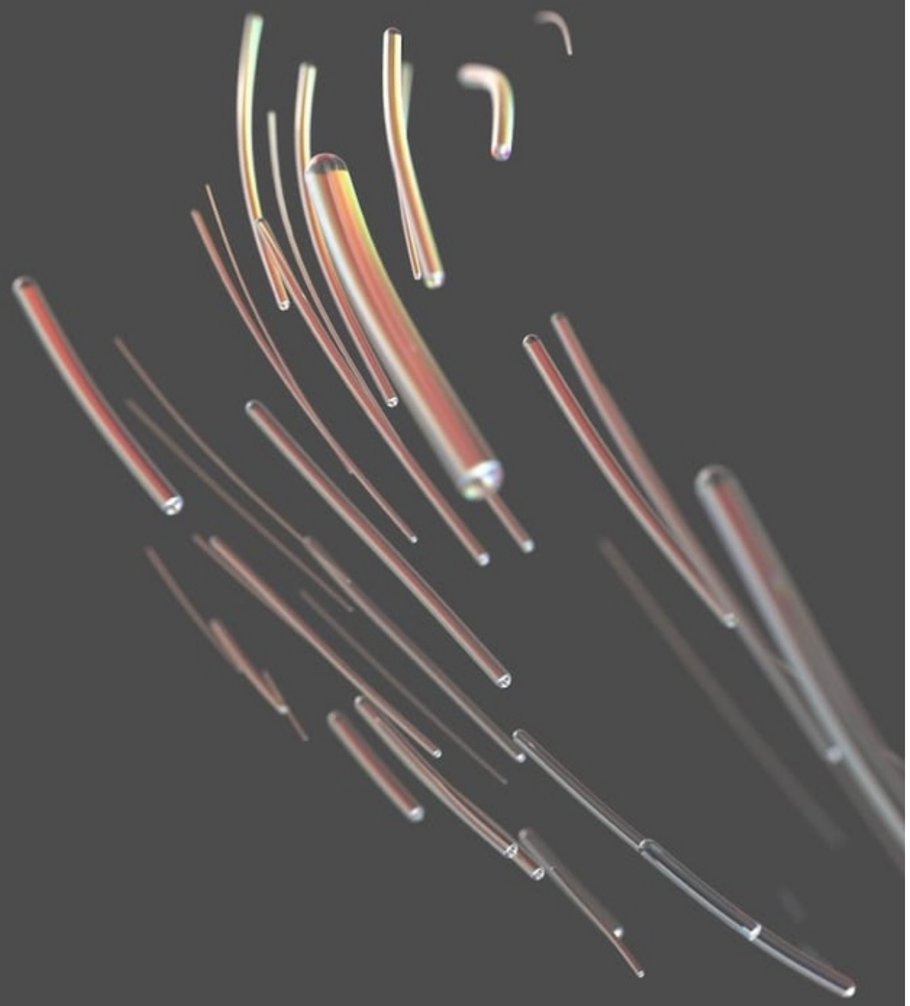


INNOQ Technology Day / 2025-11-20

SOFTWARE SUPPLY-CHAIN SECURITY

MEHR ALS NUR DEPENDENCY-MANAGEMENT

INNOQ

CHRISTOPH ISERLOHN
SENIOR CONSULTANT

Triggerwarnung

KI

Adipositas

JavaScript, Node.js, NPM


„Software is eating the world“


Software-
Supply-Chain

Nach IT-Angriff: Produktionsstopp bei Jaguar Land Rover noch bis Oktober

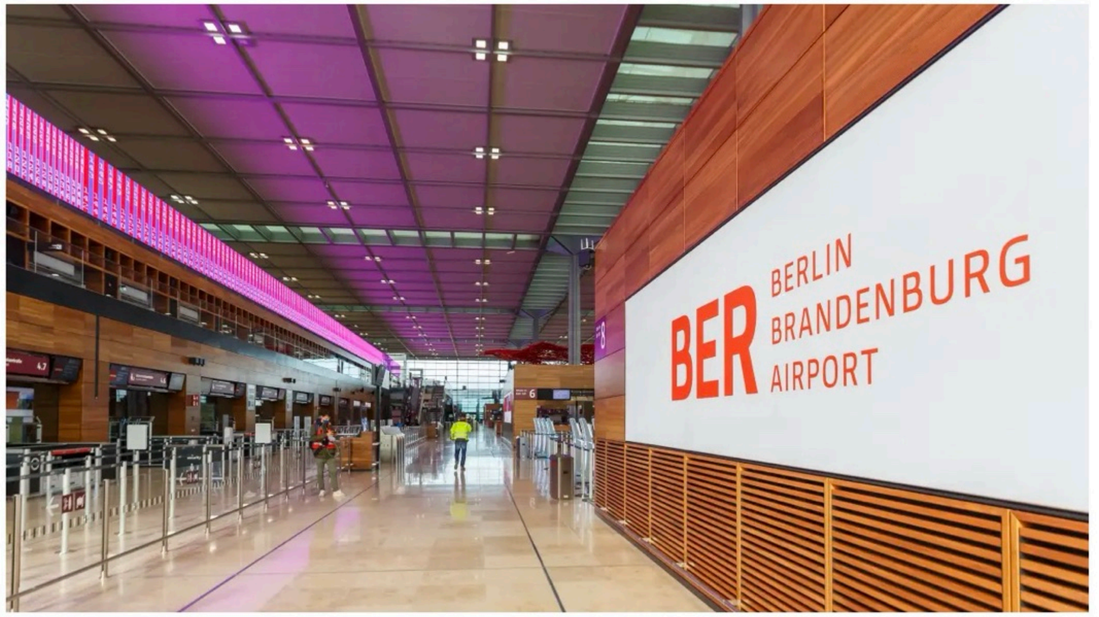
Nach einem IT-Vorfall Ende August wollte Jaguar Land Rover eigentlich in dieser Woche die Produktion wieder hochfahren. Daraus wird jetzt aber doch nichts.

(Bild: dvoevnore/Shutterstock.com)

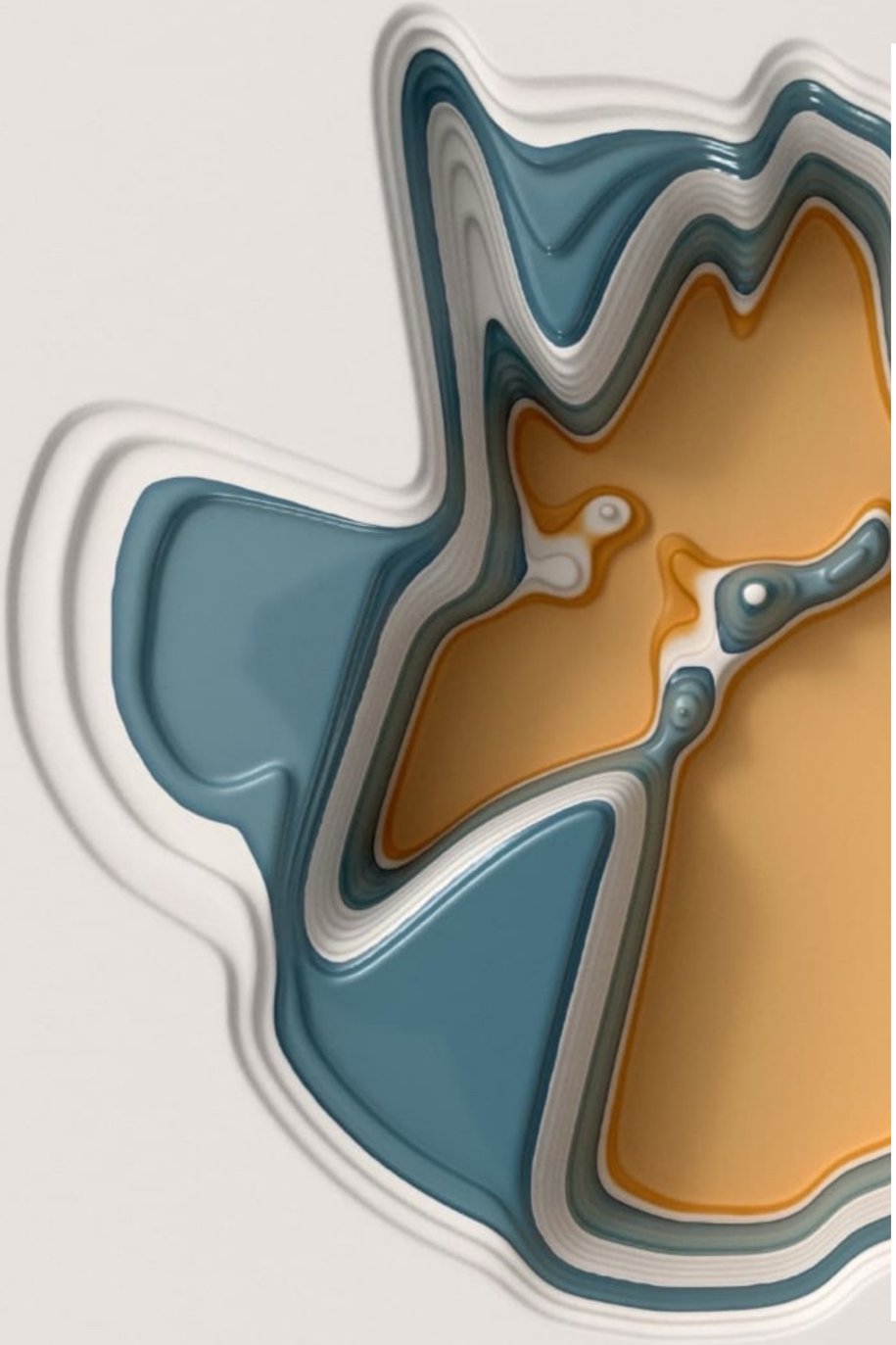
Cyberattacke auf Dienstleister behindert Flughäfen in Europa

Ein europaweiter Dienstleister für Check-in und Boarding an Flughäfen ist Opfer eines Cyberangriffs geworden. Auch der Flughafen BER ist betroffen.

64



(Bild: Markus Mainka/Shutterstock.com)



heise devSec() - Web-Security / Online / 2021-07-01

NPM

Bitte haben Sie noch einen Augenblick Geduld, der nächste Supply-Chain-Angriff ist gleich für Sie da.

INNOQ

CHRISTOPH ISERLOHN
SENIOR CONSULTANT

NUTZER GEFÄHRDET

NPM-Paket mit 5 Millionen Downloads pro Woche kompromittiert

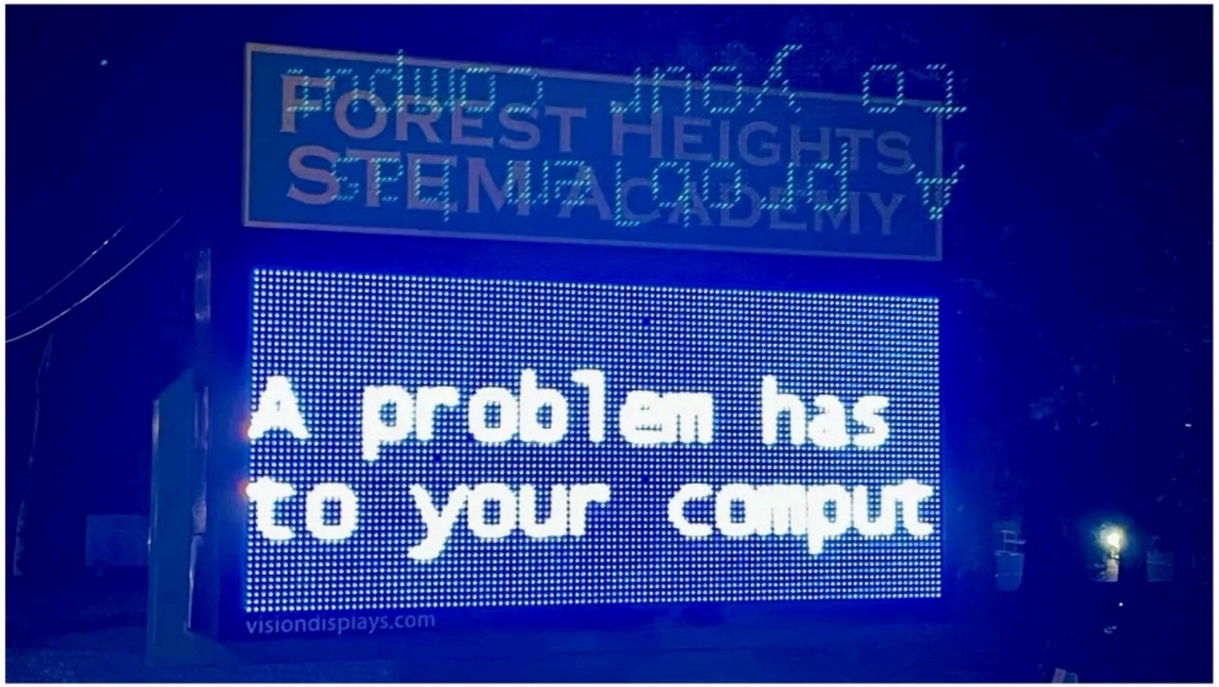
Angreifer haben Malware in ein verbreitetes Build-System namens Nx eingeschleust. Anmeldedaten zahlreicher Entwickler sollen bereits geleakt sein.

28. August 2025 um 12:15 Uhr / Marc Stöckel

```yaml
+ name: PR Title Validation
+
+ on:
+   pull_request:
+     types: [opened, edited, synchronize, reopened]
+   pull_request_target:
+     types: [opened, edited, synchronize, reopened]
+
+ jobs:
+   validate-pr-title:
+     if: ${{ github.repository_owner == 'nrwl' }}
+     name: Validate PR Title
+     runs-on: ubuntu-latest
+     steps:
+       - name: Checkout code
+         uses: actions/checkout@v4
+         with:
+           # For pull_request_target, we need to checkout the base branch
+           ref: ${{ github.event.pull_request.base.ref }}
+
+       - name: Setup Node.js
+         uses: actions/setup-node@v4
+         with:
+           node-version: 20
+
+       - name: Create PR message file
+         run: |
+           mkdir -p /tmp
+           cat > /tmp/pr-message.txt << 'EOF'
+           ${{ github.event.pull_request.title }}
+
+           ${{ github.event.pull_request.body }}
+           EOF
+
+       - name: Validate PR title
+         run: |
+           echo "Validating PR title: ${{ github.event.pull_request.title }}"
+           node ./scripts/commit-lint.js /tmp/pr-message.txt
```

Großer Angriff auf node.js

Über Spearphishing ist ein Kryptowährungsdieb in das npm-Konto eines fleißigen Entwicklers gelangt. node.js-Pakete mit Milliarden Downloads sind betroffen.



Symbolbild (Bild: Middleclasstool CC-BY-SA 4.0 Intl)

09.09.2025, 03:40 Uhr **Lesezeit: 4 Min.** | **Security**

Von Daniel AJ Sokolov

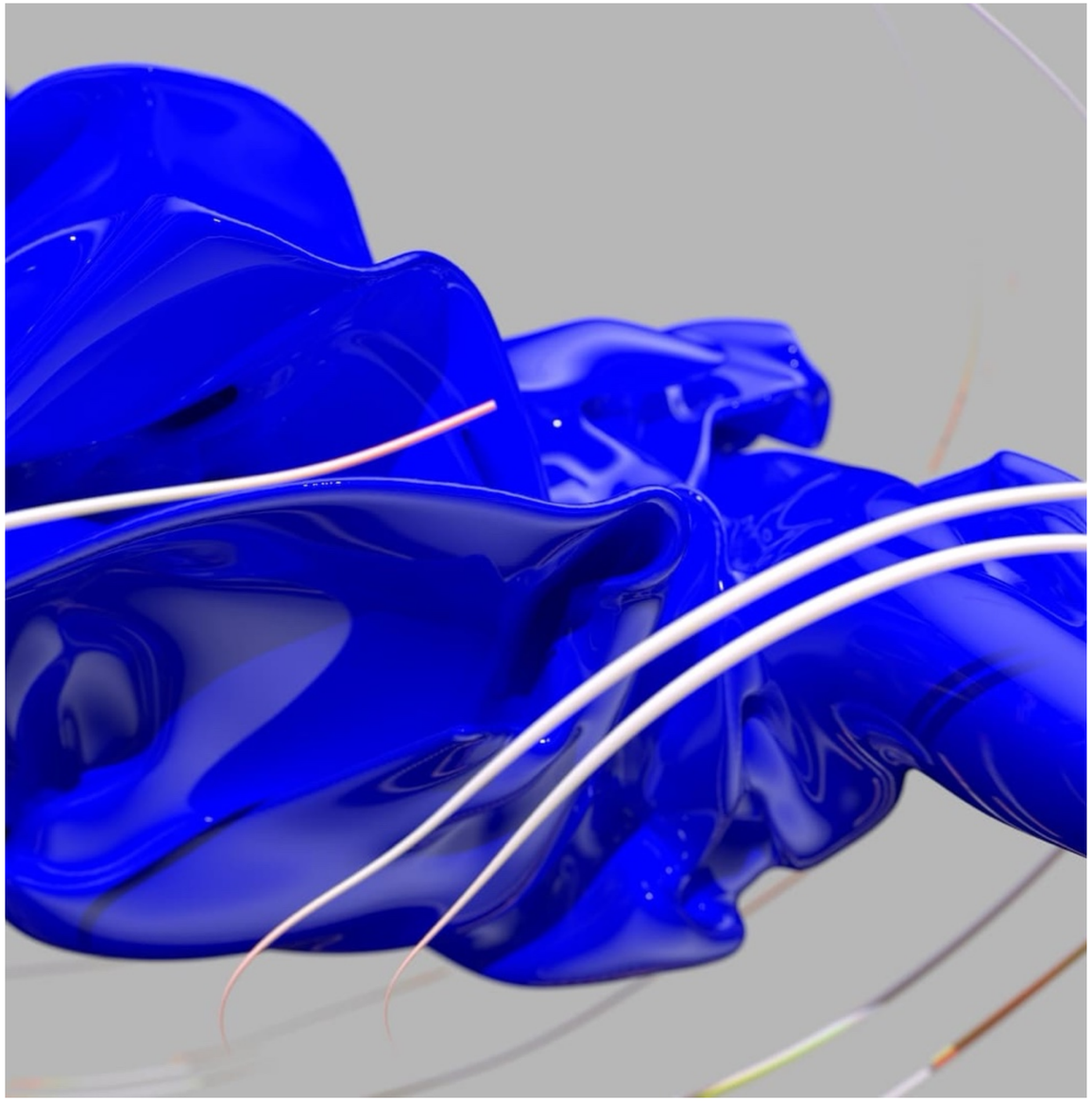
Neuer npm-Großangriff: Hunderte Pakete mit selbst-vermehrender Malware infiziert

Womöglich stecken hinter der Attacke dieselben Angreifer wie beim letzten Mal. Ihr Schadcode trägt den Namen eines prominenten Science-Fiction-Monsters in sich.

(Bild: Trismegist san/Shutterstock.com)

UPDATE 16.09.2025, 16:03 Uhr Lesezeit: 2 Min. | Security

Von Dr. Christopher Kunz



Was bisher geschah...

- Left-Pad (2016)
- Equifax (2017)
- SolarWinds (2019/2020)
- Log4Shell (2021)
- Ivanti VPN (2024)
- ...

Haben wir aktuell ein Problem?

Donnerstag, 20. November 2025

09:55 **Viele Fortinet-Produkte verwundbar, abermals Attacken auf FortiWeb**

ALERT | heise Security

09:23 **Angreifer schleusen Schadcode ein**

ALERT 52 | heise Security

Mittwoch, 19. November 2025

14:06 **Sicherheitslücken: Solarwinds Platform und Serv-U für Attacken anfällig**

ALERT | heise Security

09:50 **Support ausgelaufen: Sicherheitslücken in D-Link-Router bleiben offen**

ALERT 20 | heise Security

Dienstag, 18. November 2025

10:38 **Schadcode- und Passwortlücken bedrohen Dell ControlVault3**

ALERT 1 | heise Security

07:00 **Angriffe auf Sicherheitslücke laufen, jetzt aktualisieren**

ALERT 21 | heise Security

Warum?

Wie sieht meine Supply-Chain eigentlich aus?

Supply-Chain-Angriffe

Software Supply-Chain: Alles was die (endgültige) Software tangiert

Code/Packages, CI/CD-Systeme, Entwicklungs-Prozesse, ...

Der Hafnium Exchange-Server-Hack: Anatomie einer Katastrophe

Hätte Microsoft den Massenhack von Exchange-Servern mit rascheren Reaktionen verhindern verhindern können? Der Ablauf der Ereignisse wirft Fragen auf.

Lesezeit: 6 Min. In Pocket speichern 572

Nach NotPetya-Angriff: Weltkonzern Maersk arbeitete zehn Tage lang analog

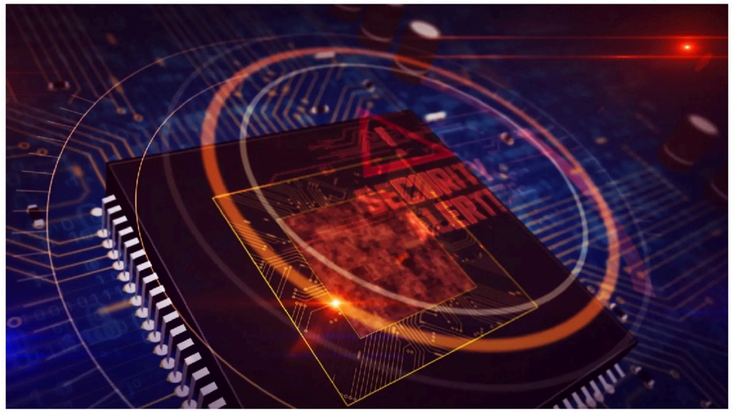
Wenn die Computer ausfallen, muss die Arbeit im Zweifel wieder auf die altmodische Art erledigt werden: mit Papier und Stift.

Lesezeit: 3 Min. In Pocket speichern 91

SolarWinds-Attacke: Ausmaß noch unklar, US-Abgeordnete diskutieren Konsequenzen

In den USA dauert die Aufarbeitung der SolarWinds-Attacke an. Im US-Senat wurde nun die Sorge laut, dass die Angreifer zurückkommen könnten.

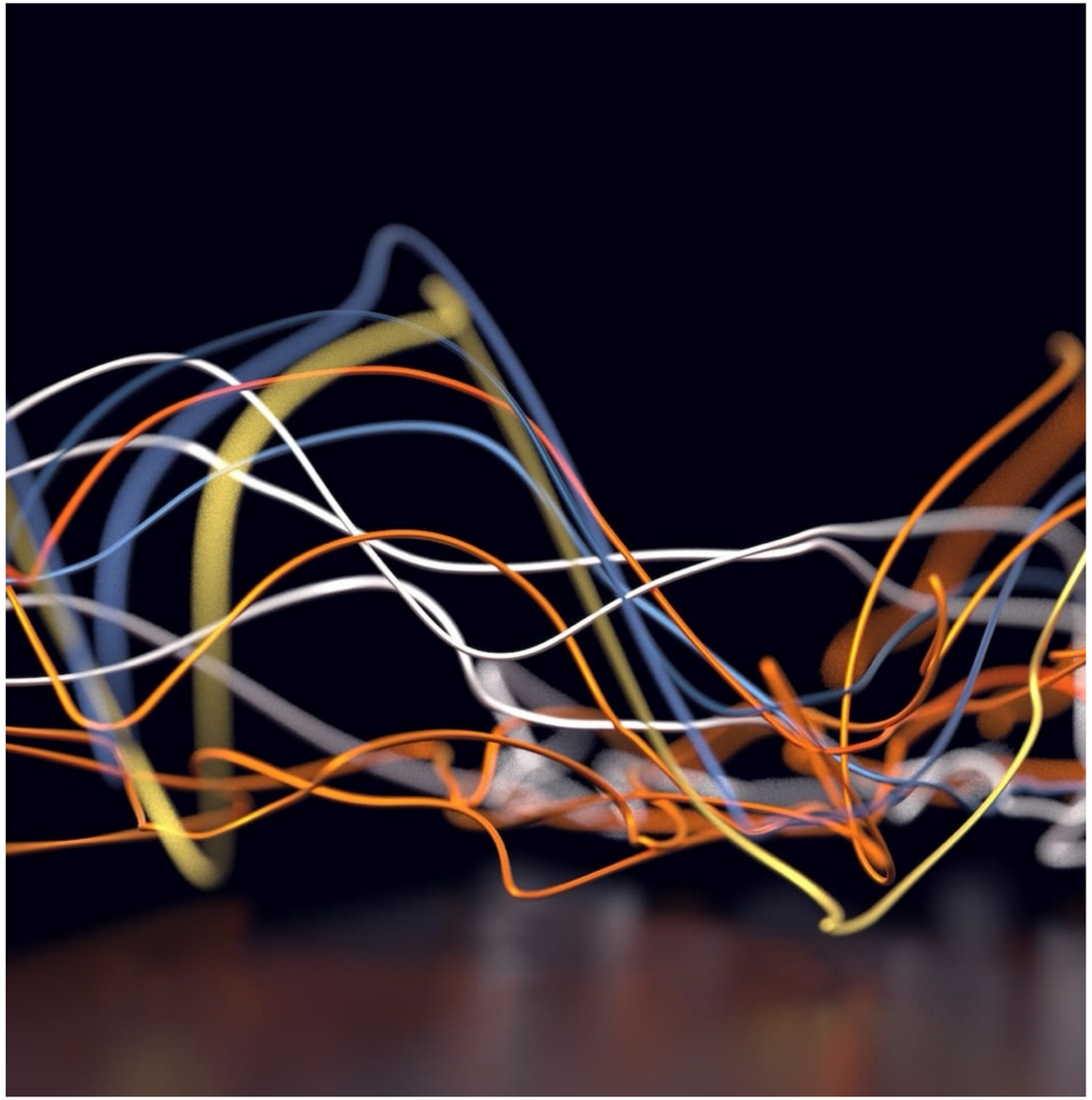
Lesezeit: 3 Min. In Pocket speichern 6



Faktoren

Cyber supply chain attack vectors*

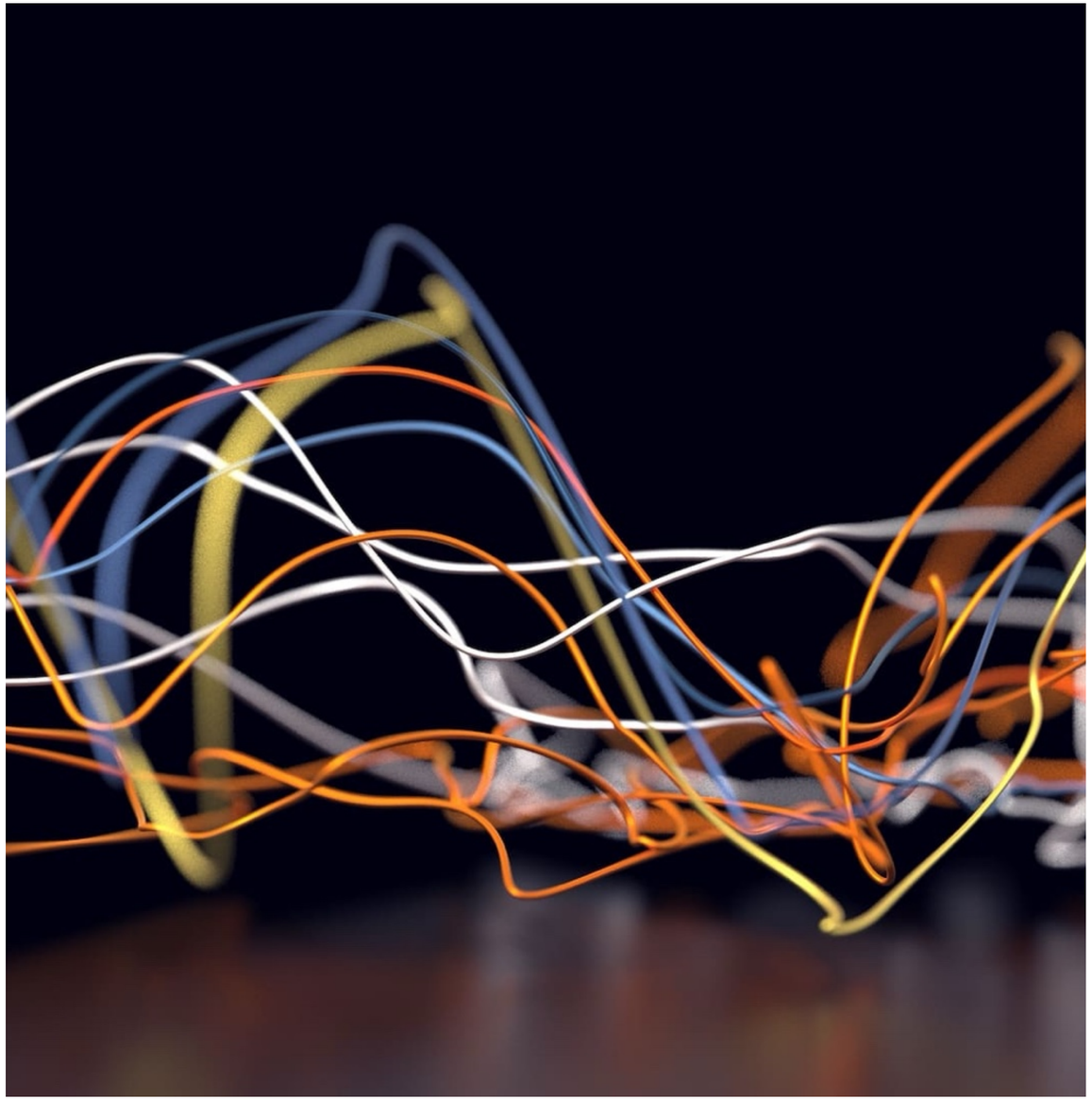
- Source Code
- Dependencies
- Build Tooling
- Deployments



* https://snyk.io/de/series/software-supply-chain-security/attacks/

Faktoren

- Kollaborations-Tools
- SaaS
- Menschen
- KI
- Machtpolitik



Wie gehen wir heute damit um?

¯_(ツ)_/¯

Vertrauen

Code-Review

Gibt es da keine Tools?

Software Supply Chain

Supply chain issues and attacks cause significant damage worldwide including lost revenue, costs of ransomware payments, costs of mitigation, denial of access to resources, reduced customer trust, and public deception.

The objective of the Supply Chain Integrity Working Group (WG) is to provide a global community for collaborating to help individuals and organizations assess and improve the security of end-to-end supply chains for open source software.

Projects

gittuf

Protect the contents of a Git repository from unauthorized or malicious changes.

Learn More

GUAC

Directed, actionable insights into the security of your software supply chain.

Learn More

Minder

Proactively manage security posture by providing a set of checks and policies.

Learn More

OpenBao

Manage, store, and distribute sensitive data including secrets, certificates, and keys

Learn More

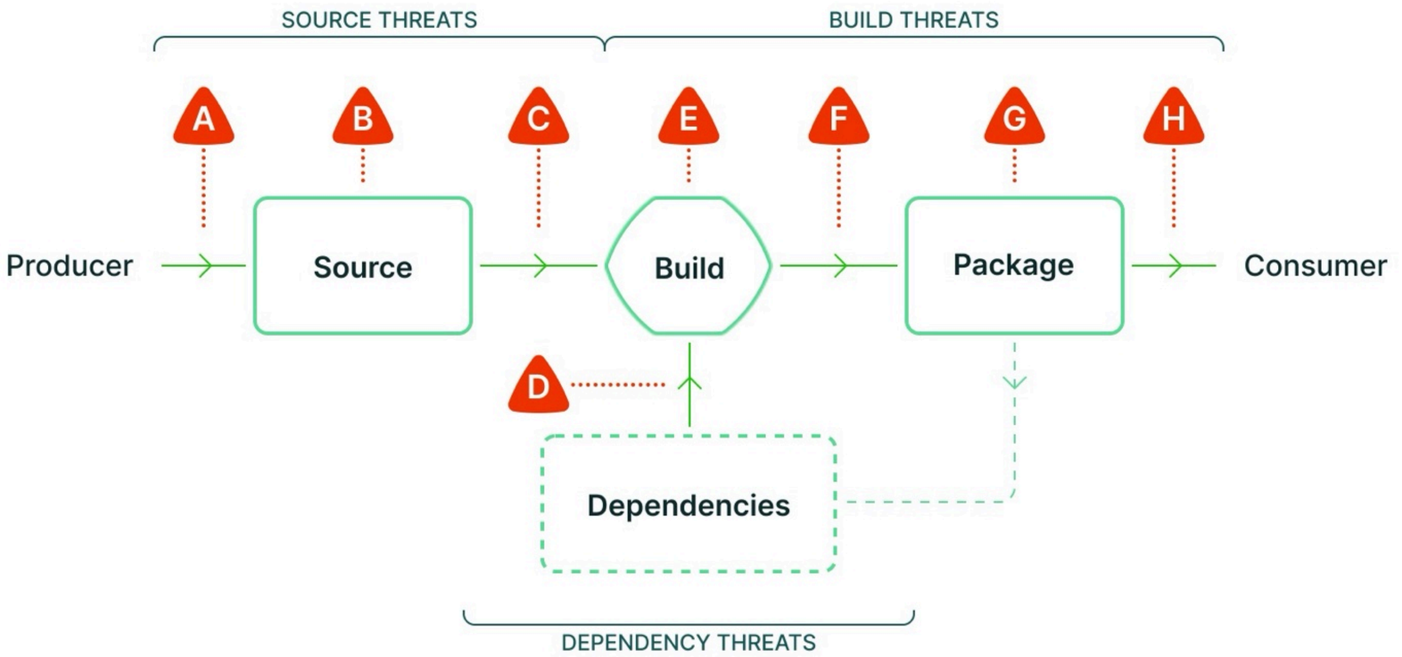
What is SLSA?

Supply-chain Levels for Software Artifacts, or SLSA ("salsa").
It's a security framework, a checklist of standards and controls to prevent tampering, improve integrity, and secure packages and infrastructure. It's how you get from "safe enough" to being as resilient as possible, at any link in the chain.

The supply chain problem

Any software can introduce vulnerabilities into a supply chain. As a system gets more complex, it's critical to already have checks and best practices in place to guarantee artifact integrity, that the source code you're relying on is the code you're actually using. Without solid foundations and a plan for the system as it grows, it's difficult to focus your efforts against tomorrow's next hack, breach or compromise.

More about supply chain attacks



SOURCE THREATS

- **A** Submit unauthorized change
- **B** Compromise source repo
- **C** Build from modified source

DEPENDENCY THREATS

- **D** Use compromised dependency

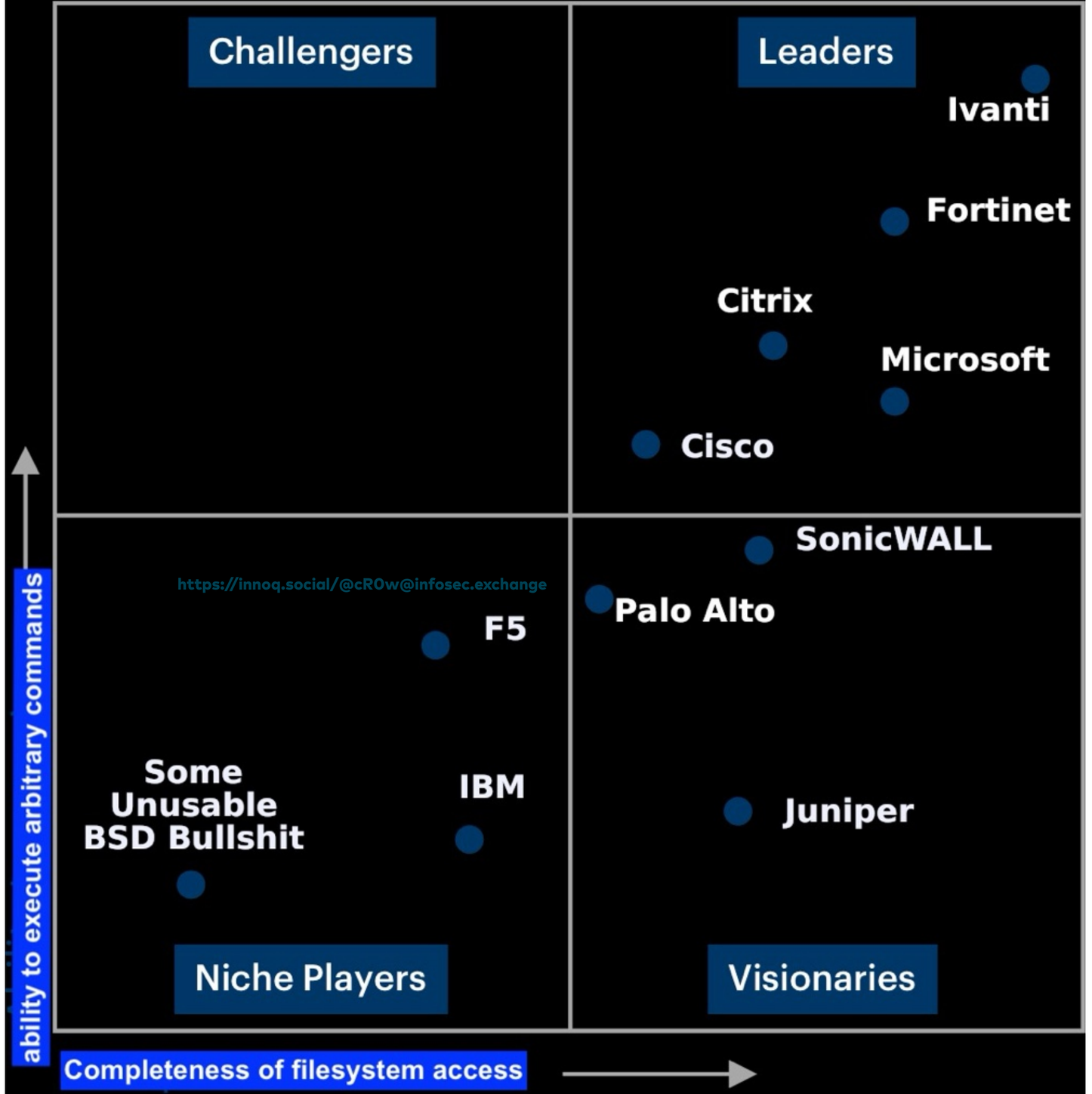
BUILD THREATS

- **E** Compromise build process
- **F** Upload modified package
- **G** Compromise package registry
- **H** Use compromised package

Reduce Supply Chain Risk

Continuous SBOM Analysis Platform

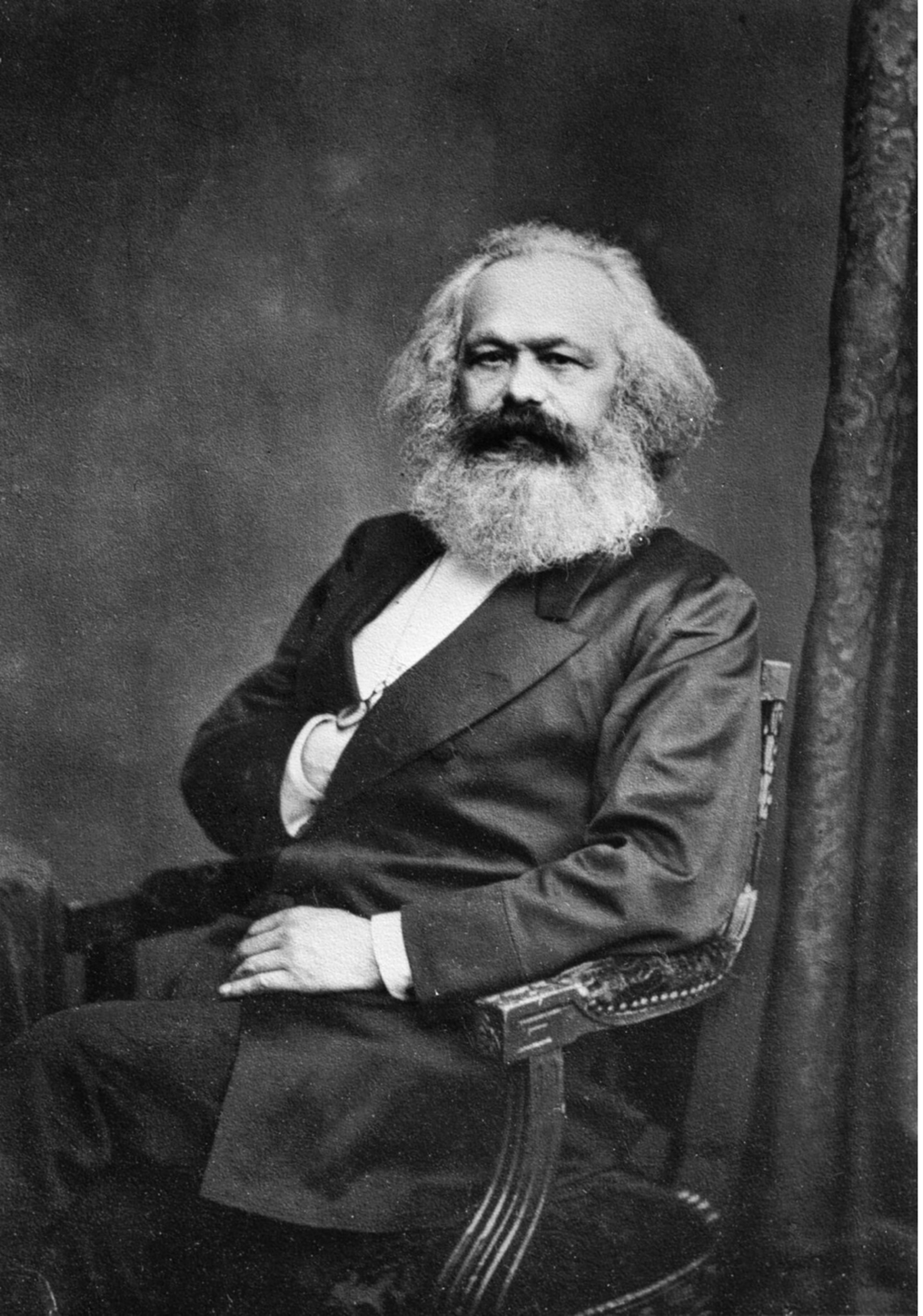
Download v4.10



https://innoq.social/@cR0w@infosec.exchange

Menschen

Ignoriert oder Vergessen?



The Cost of NotPetya

In 2017, the malware NotPetya spread from the servers of an unassuming Ukrainian software firm to some of the largest businesses worldwide, paralyzing their operations. Here's a list of the approximate damages reported by some of the worm's biggest victims.

$870,000,000

Pharmaceutical company Merck

$400,000,000

Delivery company FedEx (through European subsidiary TNT Express)

$384,000,000

French construction company Saint-Gobain

$300,000,000

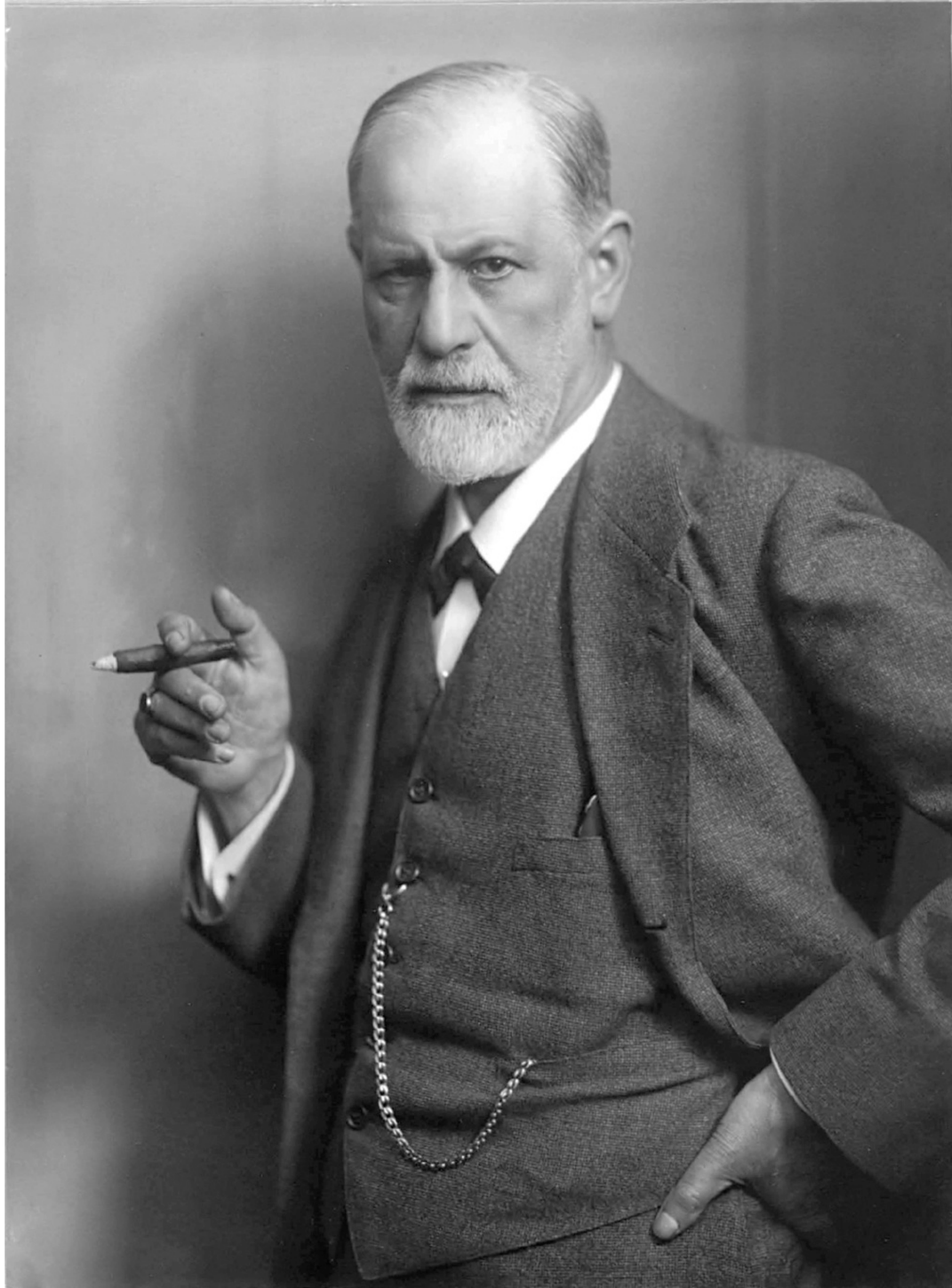
Danish shipping company Maersk

$188,000,000

Snack company Mondelēz (parent company of Nabisco and Cadbury)

$129,000,000

British manufacturer Reckitt Benckiser (owner of Lysol and Durex condoms)



IT-SICHERHEIT IN DEUTSCHLAND

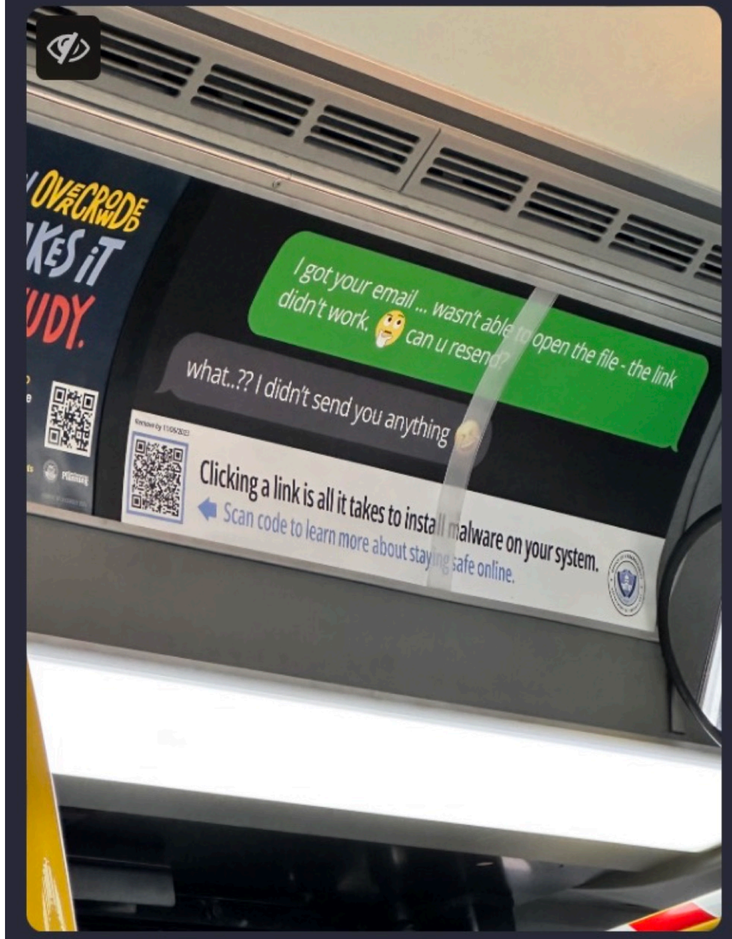
Viele Mitarbeiter missachten bewusst Security-Regeln

Einer Studie zufolge ignorieren rund zwei Drittel aller deutschen Angestellten am Arbeitsplatz bewusst gängige Sicherheitspraktiken – meistens aus reiner Bequemlichkeit.

28. Februar 2024, 13:15 Uhr, Marc Stöckel

Drew Schuster 8. Feb.
@nuncamind@xoxo.z...

Never click links!!
Also: click this link to learn more



A Sneaky Phish Just Grabbed my Mailchimp Mailing List

25 MARCH 2025

Sindre Sorhus

Oct 25, 2018 · 3 min read · Listen

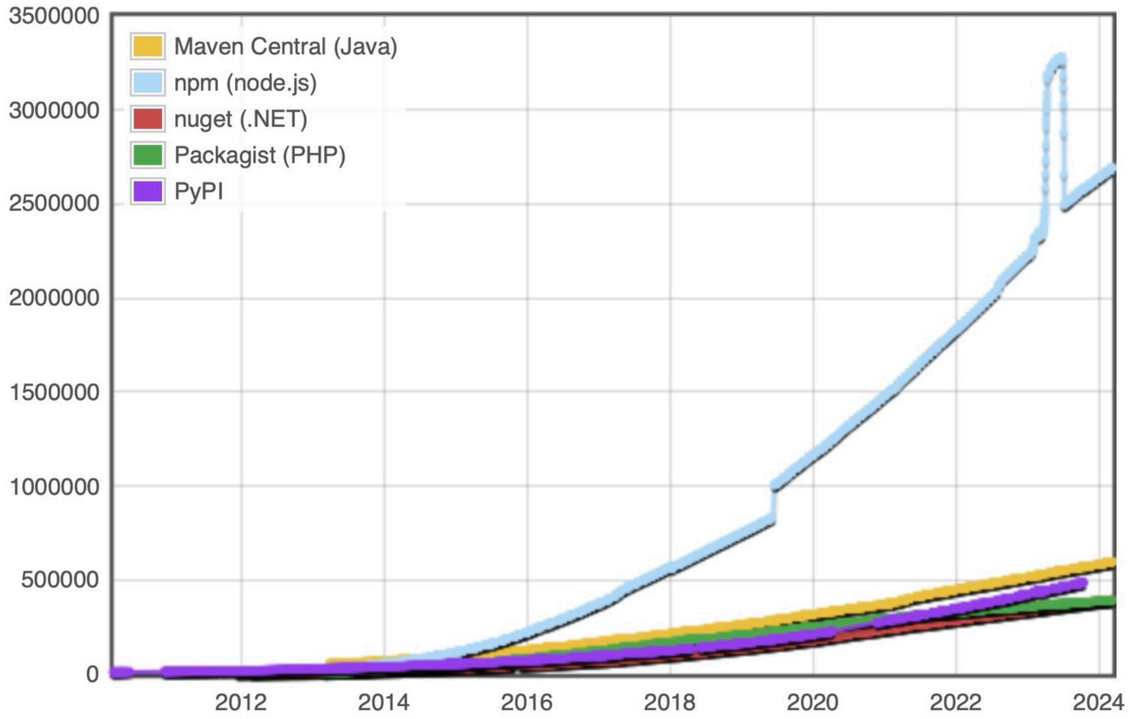
Small Focused Modules

Make small focused modules for reusability and to make it possible to build larger more advanced things that are easier to reason about.

People get way too easily caught up in the LOC (Lines Of Code). LOC is pretty much irrelevant. It doesn't matter if the module is one line or hundreds. It's all

https://medium.com/sindre-sorhus/small-focused-modules-9238d977a92a

Module Counts



(Kultur - Symbolfoto)

KI

Do Users Write More Insecure Code with AI Assistants?

Neil Perry, Megha Srivastava, Deepak Kumar, Dan Boneh

We conduct the first large-scale user study examining how users interact with an AI Code assistant to solve a variety of security related tasks across different programming languages. Overall, we find that participants who had access to an AI assistant based on OpenAI's codex-davinci-002 model wrote significantly less secure code than those without access. Additionally, participants with access to an AI assistant were more likely to believe they wrote secure code than those without access to the AI assistant. Furthermore, we find that participants who trusted the AI less and engaged more with the language and format of their prompts (e.g. re-phrasing, adjusting temperature) provided code with fewer security vulnerabilities. Finally, in order to better inform the design of future AI-based Code assistants, we provide an in-depth analysis of participants' language and interaction behavior, as well as release our user interface as an instrument to conduct similar studies in the future.

Auto generated comments #39754

Code

Closed **codemakerai-dev** wants to merge 2 commits into `spring-projects:main` from `jmnarloch:codemakerai/auto-generated-comments`

Conversation 9 | Commits 2 | Checks 0 | Files changed 3,158 | +106,277 −163

Changes from **all commits** | **File filter** | **Conversations** | 0 / 3158 files viewed | Review in codespace | Review changes

Filter changed files

buildSrc/src/main/java/org/springf...

The diff you're trying to view is too large. We only load the first 3000 changed files.

feat(repo): add GitHub Actions workflow to validate PR titles #32458

Code

Merged AgentEnder merged 1 commit into `master` from `feat/pr-title-validation` on Aug 21

Conversation 3 | Commits 1 | Checks 7 | Files changed 1 | +38

Commits on Aug 21, 2025

feat(repo): add GitHub Actions workflow to validate PR titles

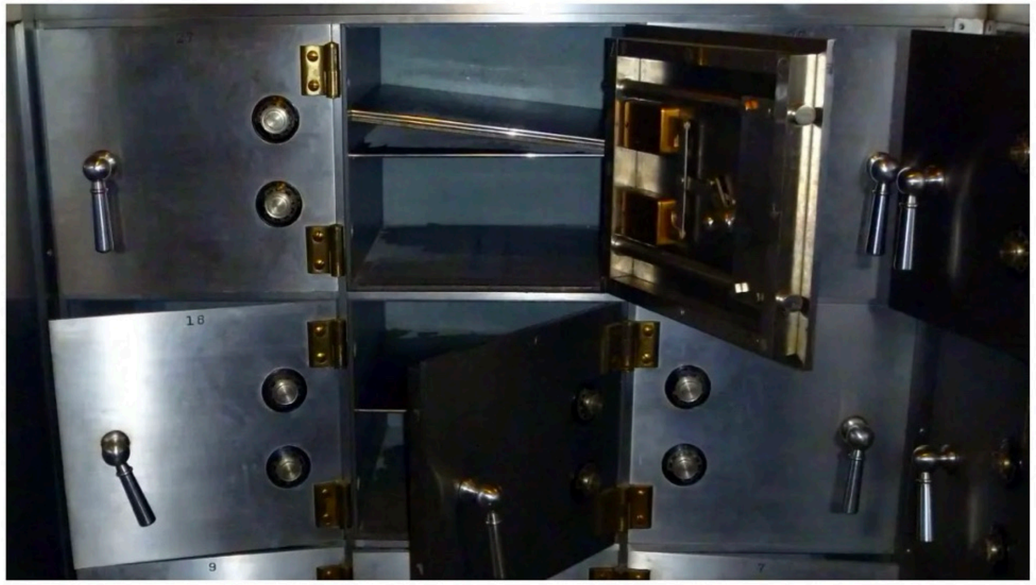
AgentEnder and claude committed on Aug 21 · ✓ 6 / 7

d994d90

Machtpolitik

US-Kürzungen: CVE-Liste könnte sofort stoppen

Die CVE-Liste ist zentral für koordinierte Maßnahmen gegen gefährliche Bugs. Die US-Regierung entzieht die Finanzierung. Per sofort.



Wäre für IT-Sicheheit noch ein Groschen da? (Bild: Daniel AJ Sokolov)

16.04.2025, 02:16 Uhr **Lesezeit: 4 Min.** | **Security**

Von Daniel AJ Sokolov

Strafgerichtshof: Microsofts E-Mail-Sperre als Weckruf für digitale Souveränität

Microsoft hat nach Trump-Sanktionen das Mail-Konto des Chefanklägers des Internationalen Gerichtshofs blockiert. Kritiker: "Wir brauchen dringend Alternativen."

693

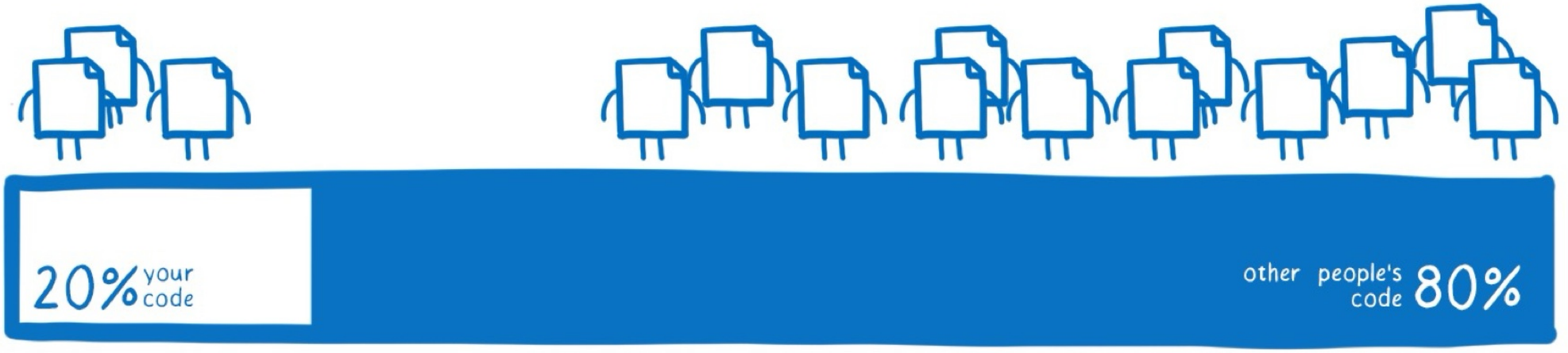
Der internationale Strafgerichtshof in Den Haag. (Bild: ICC)

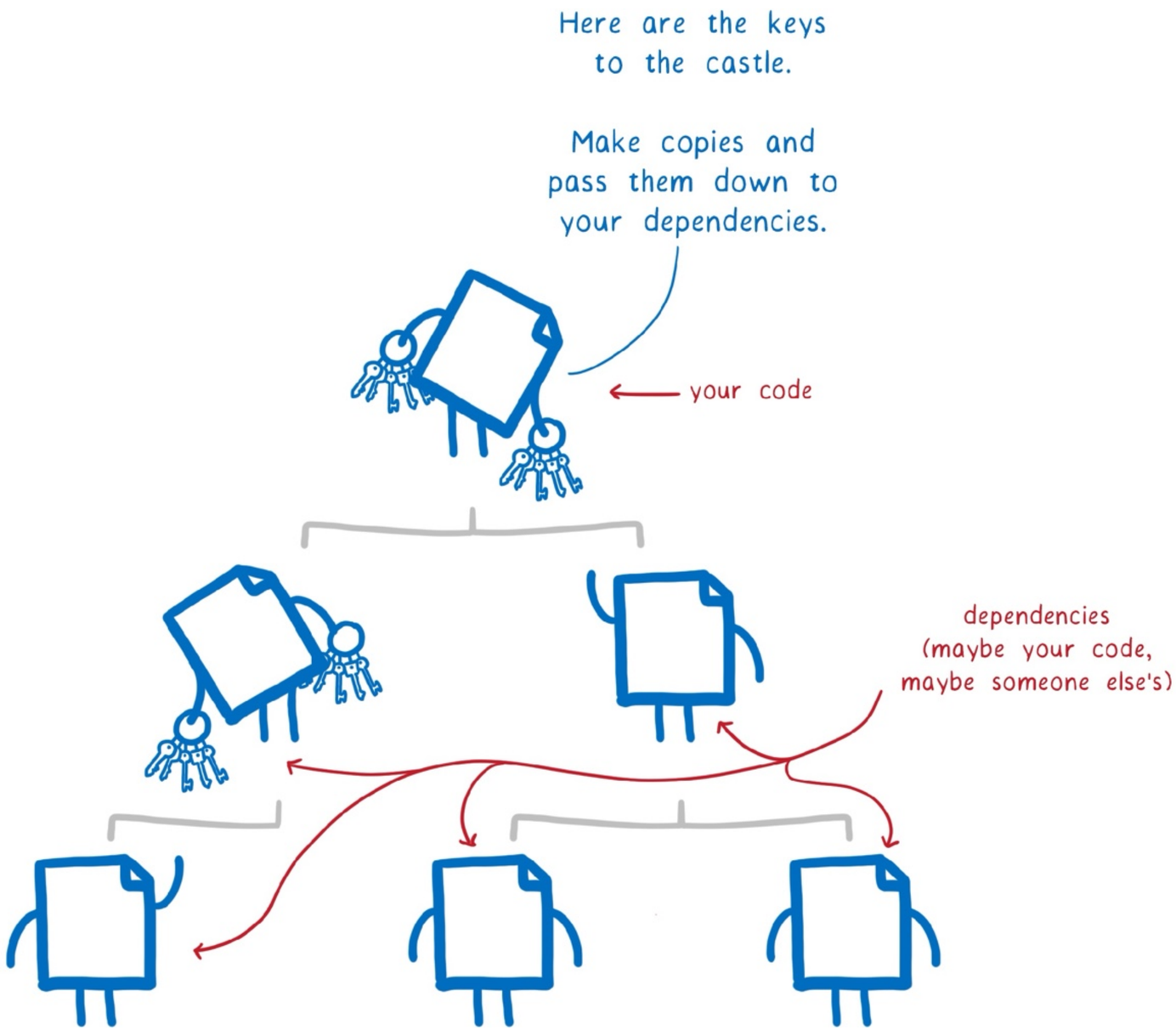
18.05.2025, 10:49 Uhr Lesezeit: 3 Min.

Von Stefan Krempl

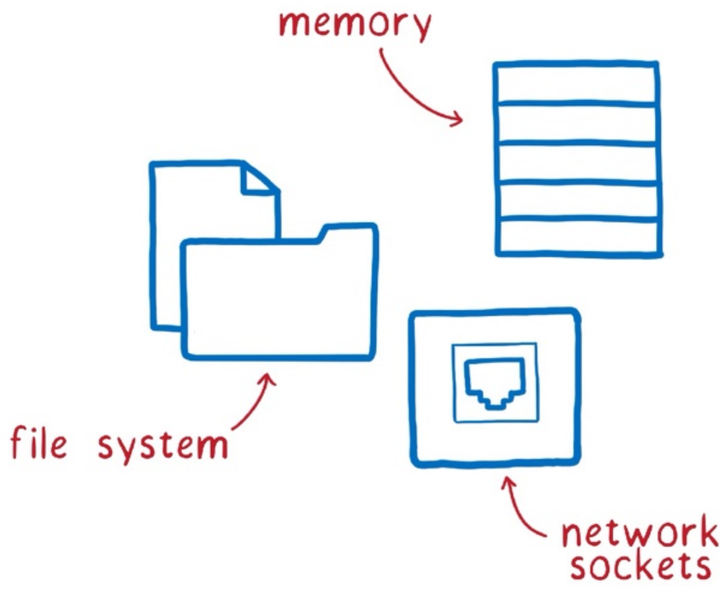
Und nun?

composition of an average code base

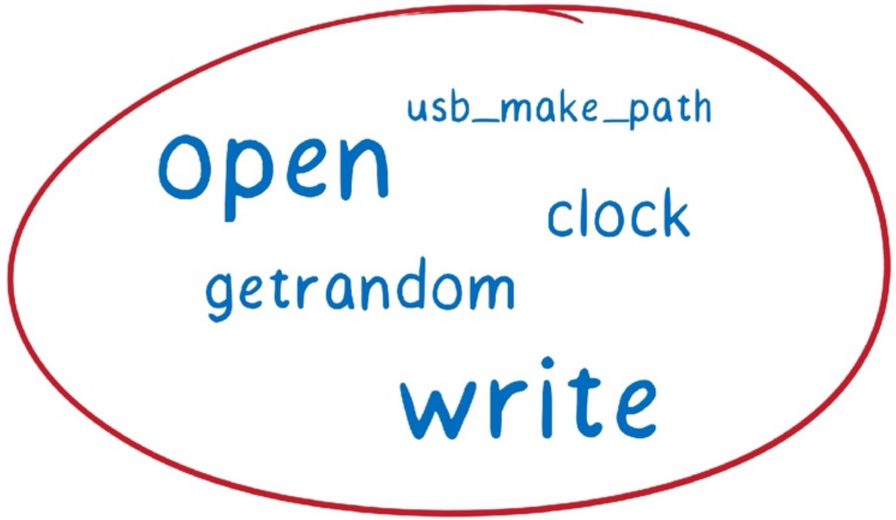


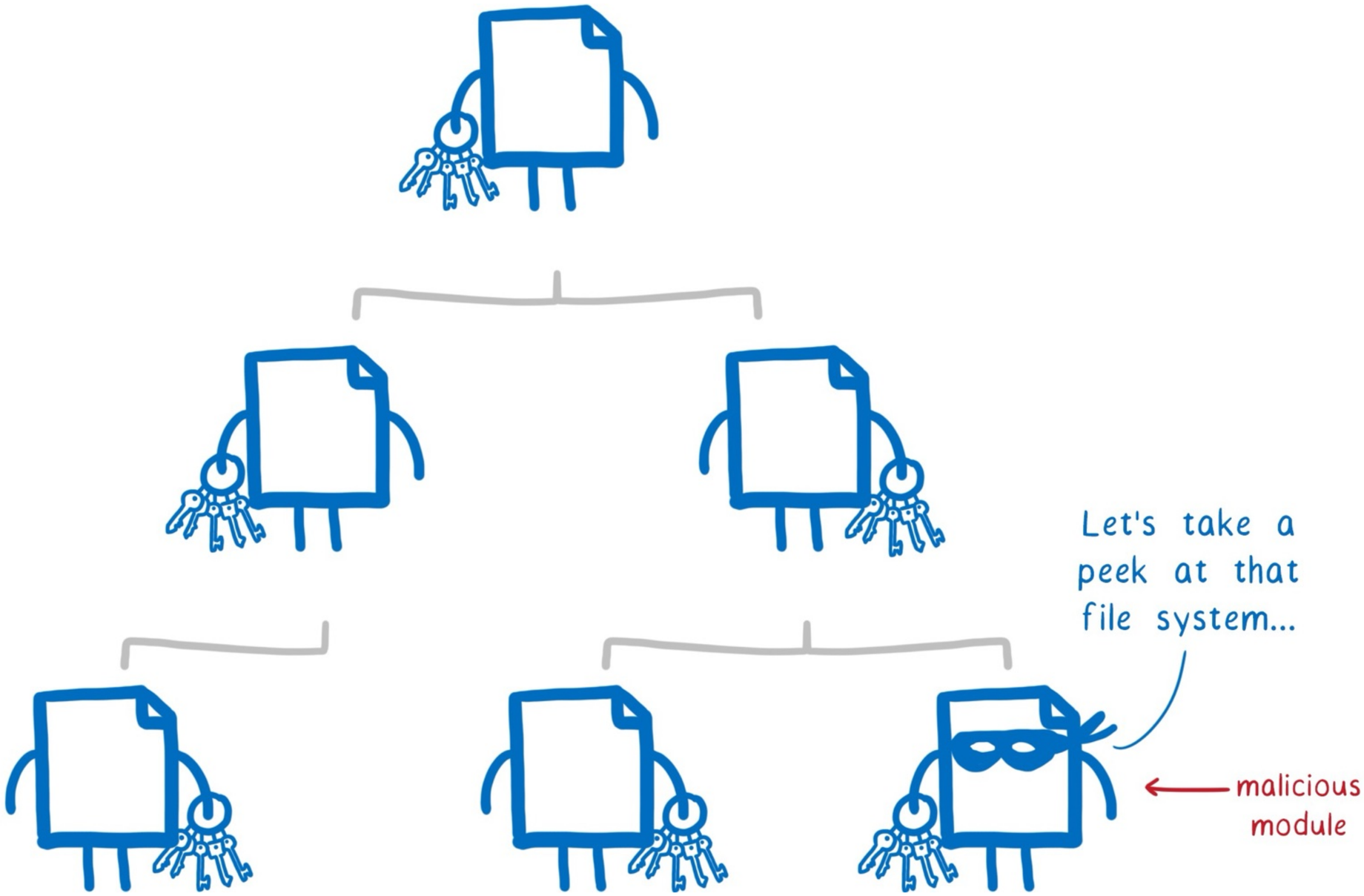


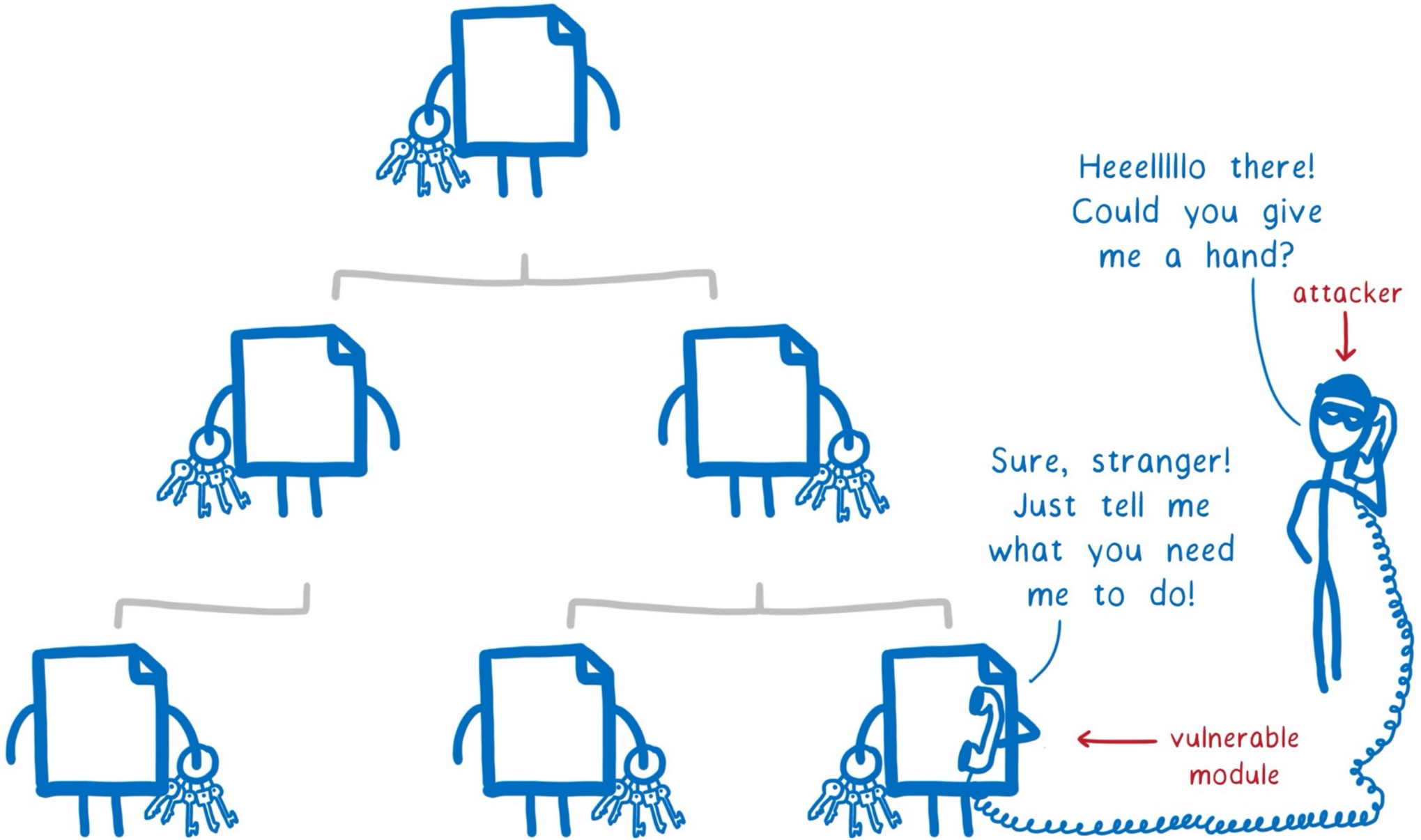
system resources



host-provided APIs & syscalls








WA

Was ist mit den nicht technischen Faktoren?

KI

NEWS | ARTIFICIAL INTELLIGENCE

The Internet Isn’t Completely Weird Yet; AI Can Fix That

“Model collapse” looms when AI trains on the output of other models

BY MATTHEW S. SMITH | 23 JUN 2023 | 5 MIN READ |

DEUTSCHE BANK WARNT

Nur KI-Blase hält US-Wirtschaft noch zusammen

Die KI-Blase werde bald platzen, warnt die Deutsche Bank. Sie generiere nicht genug Einnahmen, um die benötigte Rechenleistung aufrechtzuerhalten.

28. September 2025 um 10:50 Uhr / Mike Faust

Menschen

Heutige Software

(Symbolbild)

„There is no glory in prevention“

A Plea for Lean Software

Niklaus Wirth
ETH Zürich

Memory requirements of today's workstations typically jump substantially—from several to many megabytes—whenever there's a new software release. When demand surpasses capacity, it's time to buy add-on memory. When the system has no more extensibility, it's time to buy a new, more powerful workstation. Do increased performance and functionality keep pace with the increased demand for resources? Mostly the answer is no.

OPINION | COMPUTING

Why Bloat Is Still Software's Biggest Vulnerability › A 2024 plea for lean software

BY BERT HUBERT | 08 FEB 2024 | 10 MIN READ |

Lean Software

Beschränkte Hardware erfordert schlanke Software.

- 2 MHz Taktfrequenz
- ≈ 2 KB RAM
- ≈ 36 KB ROM
- ≈ 2 * 65.000 LOC

Fat Software

Software dehnt sich genau in dem Maß aus, wie Hardware, die zu ihrer Ausführung zur Verfügung steht.

- 1 GHz Taktfrequenz
- ≈ 1 GB RAM
- ≈ 500 MB Hard Drive Space
- ≈ 60.000.000 LOC

Software-BMI

(LOC / Features²)

Und Deine Software?

- Normalgewicht
- Präadipositas
- Adipositas Grad I
- Adipositas Grad II
- morbide Adipositas

Die fetten Jahre sind vorbei!
(hoffentlich)

Was könnt ihr tun?

Danke! Fragen?

Christoph Iserlohn
christoph.iserlohn@innoq.com
@ci@innoq.social

INNOQ
www.innoq.com

innoQ Deutschland GmbH

Krischerstr. 100
40789 Monheim
+49 2173 3366-0

Ohlauer Str. 43
10999 Berlin

Ludwigstr. 180E
63067 Offenbach

Kreuzstr. 16
80331 München

Wendenstraße 130
20537 Hamburg

Spichernstraße 44
50672 Köln